Sumo Logic Security Analytics

Security & Compliance Solutions for the Cloud & Modern IT

Tafi Makamure, Sales Engineer | Oct ‘19

Challenges With Security Monitoring Tools

Difficult to secure modern architecture	DevSecOps	▶	Need for common platform
Inability to assess threats	Cloud & app security	▶	New surface areas, threats, compliance
Too many point products	Hybrid IT	▶	Increased complexity
Alert fatigue	Security stack	▶	Ephemeral, many components
Can’t scale easily	Multi-tenant cloud	▶	New operational model

Cloud Security & Compliance Challenges

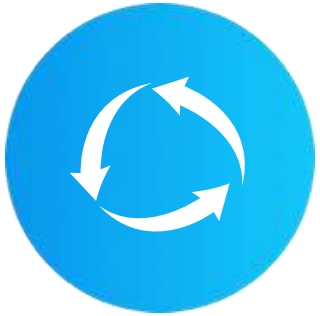
Global market challenges*

Lack of Visibility

82%

Need more App & Infra context

Legacy Silos



87%

Dramatic increase in collaboration required

Data Overload

51%

Cloud staff overloaded

Growing Skills Gaps

63%

Requires broader technical expertise

sumo logic

(*Sumo Logic Global Cloud Security Survey)

Sumo’s Security Analytics for Modern IT

Cloud & Modern App Fluent

Rapid full stack insights (App & Infra)

SaaS Architecture

Elastic scale + Rapid adoption & TTV

Integrated Workflow & Analytics

IT & Security Collaboration

Cloud Scale Analytics & Insights

10X Accelerated threat detection & response cycles

Secure Core

Platform security & compliance leader

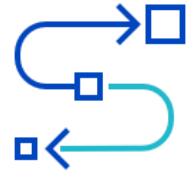
“Life before I had Sumo Logic was absolutely frustrating - I had no visibility into what was happening in my security environment.”

Milinda Rambel Stone, Director of Security @ SPS Commerce

Why Sumo for Security Monitoring/ Analytics/ SIEM?

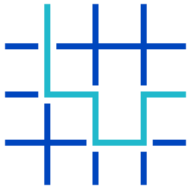
Unified: Security View of Hybrid, Multicloud

Cloud Scale: Grow without Capacity Planning



Cloud Economics: Utility based Consumption Model

Tool Consolidation: One tool for SecOps, ITOps, DevOps



Analytics-Driven: Manage big data on cloud easily

Platform Security: FedRAMP Ready, PCI/ HIPAA certified, End-to-end encryption

Sumo Security Analytics - Cloud SIEM

Hybrid IT

IaaS/ PaaS/ SaaS

Apps/ Microservices

User Security

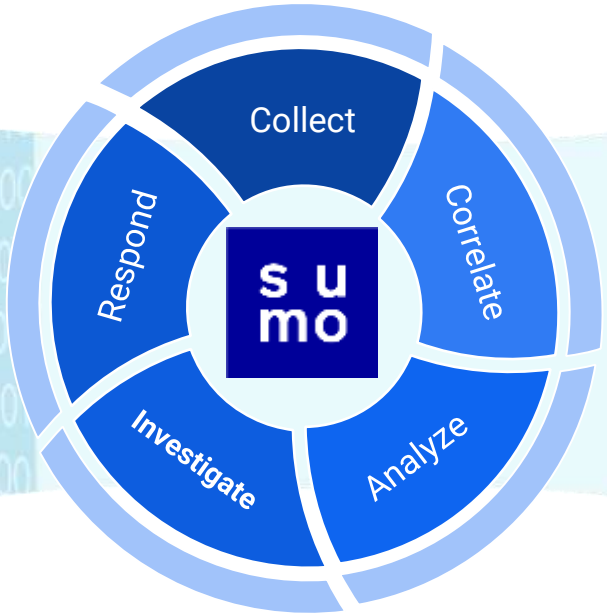
Apps Security

Network Security

Data Security

Structured | Unstructured

Logs | Events



Detect | Respond

SecOps

CISO

Architects

Dir of Security

Risk

Sec Analyst

Compliance

Threat Detection	Forensic investigation	Incident response
		

sumo logic

Advanced Analytics

Log Reduce

What: Reduce thousands of log lines into easily understood patterns

Value: Reduce MTTI/MTTR by up to 90%

Log Compare

What: Compare baselines before and after events

Value: Analyze migrations, across releases & environments

Outlier Detection

What: Monitor metrics & KPIs via dynamic thresholds

Value: Accurate, real-time alerting while eliminating false-positives

Predictive Analytics

What: Leverage historical data to predict future trends

Value: Proactively plan to reduce risk

Forensic Investigation

Outlier Detection

What: Detects threats that need further investigation

Value: Accurate, real-time alerting while eliminating false-positives

Free-form Search

What: Perform free-form search on raw or metadata

Value: Quick search tool to isolate and pivot to problems

Log Compare

What: Compare baselines before and after events

Value: Analyze migrations, across releases & environments

Log Reduce

What: Reduce thousands of log lines into easily understood patterns

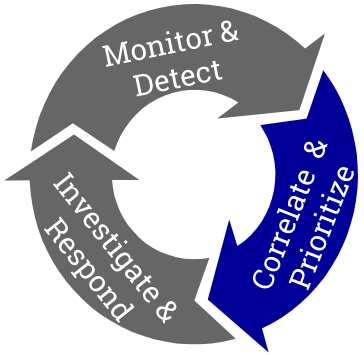
Value: Reduce MTTI/MTTR by up to 90%

Benchmarking with Global Intelligent Service

- ✓ Benchmark against peers
- ✓ know what is normal...
- ✓ Drill down on rare events that you would typically miss
- ✓ Provides statistical analysis of your threats vs. benchmark
- ✓ Get insight into your targeted sources that beats benchmark

sumo logic

Focused Full Stack Threat Correlation

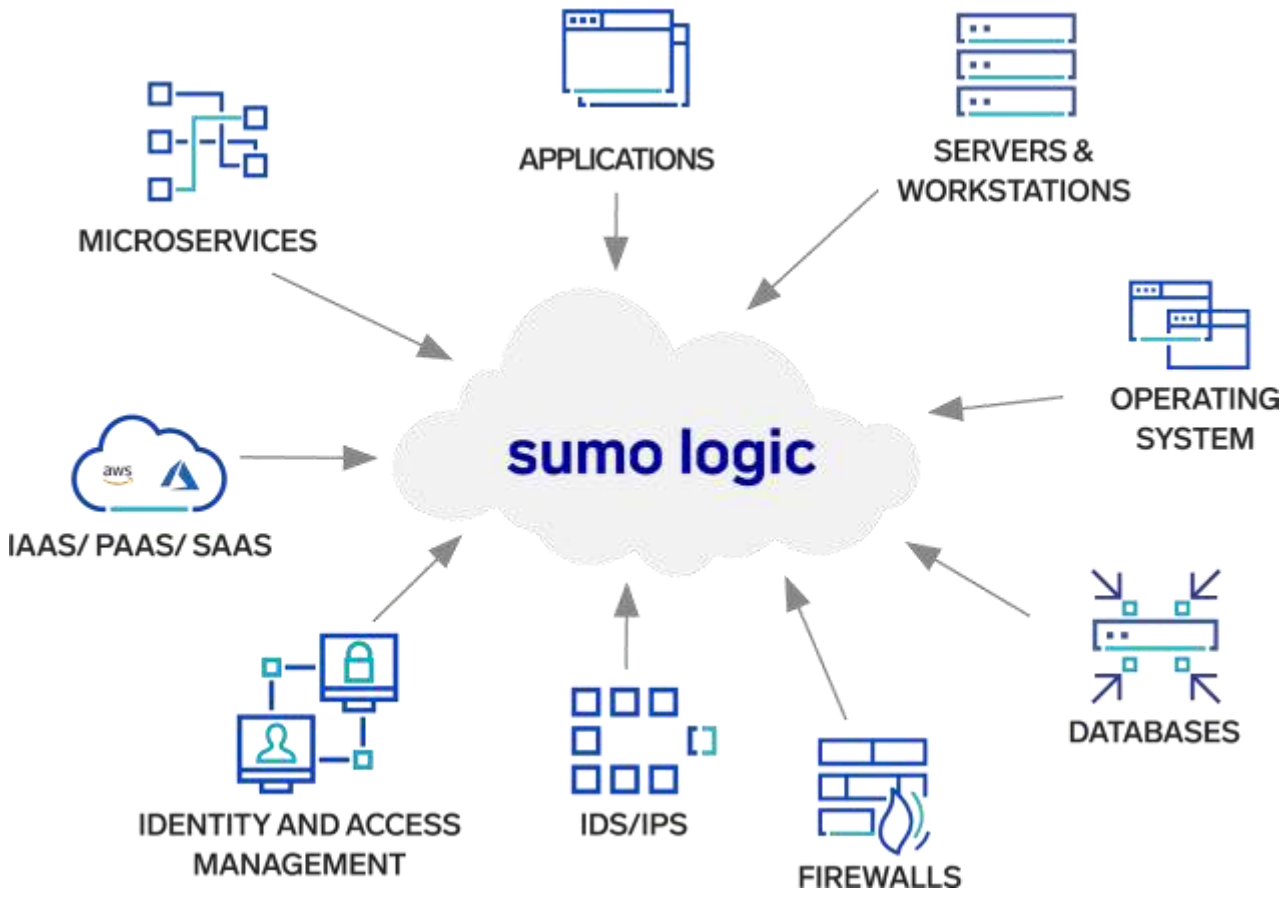


- ✓ Dynamic & targeted correlation
- ✓ Full stack (App & Infra) analytics
- ✓ Customizable alerts & alarms
- ✓ Integrated Threat Intelligence

sumo logic

Sumo Platform Compliance & Certifications

- ✓ PCI DSS 3.2 Level 1 certified
- ✓ SOC 2 Type II attestation
- ✓ ISO 27001 certified
- ✓ CSA Star certified
- ✓ HIPAA-HITECH compliance
- ✓ U.S. – EU Privacy Shield
- ✓ AES 256-bit encryption at rest
- ✓ TLS encryption in transit
- ✓ FedRAMP Ready
- ✓ CIS AWS Foundations



Unified Visibility & Control for Modern IT

Secure, Cloud-Native Data Analytics for Continuous Intelligence across All Environments

✓ Full App & Infra Insights
- Built in the Cloud for the Cloud
- Elastic Scale at Cloud Speed
- Industry Leading Secure Core Platform
- Rapid Time to Value

✓ Accelerated MTTI/MTTR
- Detect, Investigate, Respond at Cloud Speed
- Security & Compliance Enablement
- Machine Learning Data Analytics
- Beta - Intelligent Investigation Workflows

✓ Accelerated Digital Strategy
- Tool Consolidation - Fosters collaboration
- Enables Convergence of IT & Security (DevSecOps)

Sumo Customers by Vertical

Financial & Prof. Services

AVIVA, VISA, Ameriprise Financial, sage, accenture, Braintree, A PayPal Company, NEW YORK LIFE, Virgin money, PennyMac, Allianz

Travel

airbnb, Marriott HOTELS · RESORTS · SUITES, Expedia, DELTA, Alaska AIRLINES, jetBlue AIRWAYS, webjet.com, Hotel Tonight

SaaS & Cloud

salesforce, xero, CHEF, netskope, Hootsuite, Acquia, DOMO, Gainsight, twilio, zuora

Media & Entertainment

The New York Times, VIACOM, BBC, The Washington Post, Mc Graw Hill Education, SUPERCELL, MAJOR LEAGUE BASEBALL, 4 CHANNEL FOUR TELEVISION, shutterstock, HEARST corporation, News Corp Australia, CAESARS ENTERTAINMENT

(e)Retail, Industrials & Mfg

WD-40, RH, ABInBev, ebay, LAND O'LAKES, Levi's LEVI STRAUSS & CO., Copart, BED BATH & BEYOND

Gov. & Education

COLUMBIA UNIVERSITY, ABC Australian Broadcasting Corporation, Bucknell UNIVERSITY, Cabinet Office, HM Revenue & Customs, AUSTRALIA POST, WCU WEST CHESTER UNIVERSITY

Tech. & Communications

Microsoft, twitter, Adobe, GoDaddy, f5, Dome9 SECURITY, CITRIX, SAMSUNG SmartThings, SONOS

Healthcare

KAISER PERMANENTE, 23andMe, AstraZeneca, one MEDICAL GROUP, MD Anderson Cancer Network, MEDECINS SANS FRONTIERES DOCTORS WITHOUT BORDERS, medidata, MEDHOST

sumo logic

Thank you

Tafi Makamure

Sales Engineer

Email: tafi@sumologic.com

sumo logic

s u

See business differently

m o